UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/892,667	06/28/2001	Luke E. Girard	219.40075X00	2051

23838 7590 12/03/2004

KENYON & KENYON
1500 K STREET, N.W., SUITE 700
WASHINGTON, DC 20005

EXAMINER	
POLTORAK, PIOTR	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 12/03/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/892,667	GIRARD, LUKE E.	
	Examiner	Art Unit	
	Peter Poltorak	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 June 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-26 have been examined.

Priority

2. The effective filing date for the subject matter defined in the pending claims in this application is 06/28/2001.

Drawings

3. The drawings are objected to because of the following informalities: the number "7" used in the drawings is drawn inconsistently. For example, in Fig. 7 (the object 170) does not look similar to object 710 (?) in which the number "7" resembles the number 4.
4. Fig. 1 shows object 140 labeled "flash memory" but discusses it as "protected storage" in the specification. Fig. 2 shows object 210 labeled "protected storage". It is not clear whether objects 140 and 210 refer to the same objects.
5. The meaning of "protected storage" within object 370(?) *(Fig. 3)* and 470 (?) *(Fig. 4)* is not clear.
6. It is not clear whether the middle circle in Fig. 5 is object 510B or 5108.
7. It is not clear whether object 620 "Polic Tracking System" in Fig. 6 is meant to read as "Police Tracking System" or "Policy Tracking System".
8. Corrected drawing sheets are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure

number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

9. Claims 8 and 17 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Claims recite limitations directed towards Intel ®

Protected Access Architecture (IPAA) described in Application Interface Specification, Revision 1.0; however, no documentation is provided.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 6-14, 16-19, 21-23 and 26 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
11. The limitation "corresponds to" in claims 6, 8, 12-14, 17, 21-23 is not clear.
12. Claims 7, 16 and 26 recite different limitations followed by "or a lack of communication to a policy server or to a security token". It is not clear whether the "lack of communication" is an alternative to all the previous limitations or just to the last one.
13. Claims 7-8 and 12-14 are rejected by virtue of their dependence.
14. Appropriate correction is required.

Rejections - 35 USC § 102

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

15. Claims 1-2, 4-6 and 15, 20-22 are rejected under 35 U.S.C. 102(b) as being anticipated by *Isikoff (U.S. Patent No. 5748084)*.
16. As per claim 1 *Isikoff* teaches a host chipset *(see Fig. 4),* a beacon equipped laptop computer configured for operating within a terrestrial cellular network *(Fig. 1 and col. 3 lines 5-7),* and teaches that transmission of radio waves

allow to pinpoint the location of the device which reads on a (RF-based) locator subsystem connected to the host chipset and arranged to determine a current location of the mobile system. Laptops inherently have main storage connected to the host chipset and arranged to store an operating system (OS) and contain an OS-Present application and/or a Pre-OS application configured to enforce security policies during user authentication. *Isikoff* teaches enforcing security policies during user authentication, accessing the locator subsystem and determining whether the mobile system may have been stolen or used inappropriately based on the security policies *(col. 5 lines 6-11)*.

17. As per claim 2, laptops inherently have main memory to store OS, and the OS-Present application and flash memory to store Pre-OS application are executed during boot up. *Isikoff* shows main memory in Fig. 4 and teaches BIOS *(col. 6 lines 26-27)*.

18. As per claim 5, a hard drive *(Fig. 4)* is a non-volatile readable and writeable memory device.

19. Claim 15 is substantially equivalent to claims 1-2; therefore claim 15 is similarly rejected.

20. As per claim 20-22, *Isikoff* teaches the mobile device using a GPS receiver and the transmitter transmitting its position coordinates (*Isikoff,* col. 10 lines 20-29). Also, *Isikoff* teaches reporting a violation to an OS readable location in the protected storage and/or an external event monitoring facility *(col. 5 lines 8-33, col. 3 lines 30-35, col. 4 lines 14-16)*. The *Isikoff's* beacon

equipped laptop configured for operating within a terrestrial cellular network, represented by relay station 110 as shown in Fig. 1 *(col. 3 lines 5-7)* reads on the RF-based locator providing location based information is via a radio tower, for enabling the police to track and recover the stolen device.

21. Claim 24 is rejected under 35 U.S.C. 102(b) as being anticipated by *Cromer et al. (U.S. Patent No. 6166688).*

22. The preamble of claim 24 recites "configured in accordance with Intel ® Protected Access Architecture". However, since no documentation on IPAA has been provided, the limitation is present only in the preamble and the claim 24 steps don't depend on the IPAA, the examiner does not address the limitation.

23. *Cromer et al.* teach a laptop *(Fig. 1)* depicting the power-on-self-test (POST) accessing EEPROM to determine if new (location) coordinates have been stored in EEPROM, which reads on processor performing initializing and testing a system platform *(Cromer et al. col. 6 lines 28-35)*. If new coordinates are found a password is used to validate the new coordinates *(col. 6 lines 35-55)*. After the verification of the coordinates the determination is made of the current geographical location which is compared with the authorized geographical area *(col. 7 lines 9-17)*. This reads on "checking a Pre-OS security policy record for an approved trigger mechanism, determining if there is a violation of security policies during user authentication. If a determination is made that a portable computer is outside the authorized area the laptop is disabled utilizing a power control signal *(col. 7 lines 23-28)*. This reads on "if

there is a violation of the security policies, making a decision that the mobile system may have been stolen or used inappropriately".

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

24. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over *Isikoff (U.S. Patent No. 5748084)* in view of Official Notice.

As per claim 3 Official Notice is taken that it is old and well-known to configure a laptop's protected storage to support the Pre-OS application and the OS-Present application and to store configuration data, the security policies, authentication data and other information obtained from the Pre-OS application and the OS-Present application.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to configure a laptop's protected storage to support the Pre-OS application and the OS-Present application and to store configuration data, the security policies, authentication data and other information obtained from the Pre-OS application and the OS-Present application. One of ordinary skill in the art would have been motivated to perform such a modification in order to assure laptop's security and integrity.

25. Claims 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over *Isikoff (U.S. Patent No. 5748084)* in view of *Bajikar (U.S. Pub. 20020194500).*

Isikoff teaches the mobile system as discussed above.

Isikoff does not teach the RF-based locator subsystem corresponding to a Bluetooth TM transceiver that is part of a Bluetooth TM based security system including a central security server and a network of Bluetooth (voice/data) Access Points (BTAPs) installed in a designated area to provide security services for the mobile system, including asset control, remote monitoring and tracking of the mobile system, through the Internet or the RF-based wireless network.

Bajikar teaches a Bluetooth based security system utilized to provide ad-hoc security services to secured assets comprising a secured device (SD) equipped with Bluetooth (BT) technology; a plurality of Bluetooth Access Points (BTAPs) located at designated points to establish a BT link with the secured device (SD); and a security server (SS) connected to all BTAPs and arranged to provide access control and security services for the secured device (SD), wherein the security server (SS) obtains attribute information *(Abstract and Fig. 1)*. Furthermore *Bajikar* discloses that the Bluetooth TM based security system serves to control and monitor the status of all secured devices or assets remotely, through the Internet or other networks *[0024]*.

The *Bajikar's* teaching reads on RF-based locator subsystem corresponding to a Bluetooth TM transceiver that is part of a Bluetooth TM based security system including a central security server and a network of Bluetooth

(voice/data) Access Points (BTAPs) installed in a designated area to provide security services for the mobile system, including asset control, remote monitoring and tracking of the mobile system, through the Internet or the RF-based wireless network.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to utilize an RF-based locator subsystem subsystem corresponding to a Bluetooth TM transceiver that is part of a Bluetooth TM based security system including a central security server and a network of Bluetooth (voice/data) Access Points (BTAPs) installed in a designated area to provide security services for the mobile system, including asset control, remote monitoring and tracking of the mobile system, through the Internet or the RF-based wireless network as taught by *Bajikar.* One of ordinary skill in the art would have been motivated to perform such a modification in order to provide low-cost and low-power ad-hoc security *[Bajikar 0021].*

26. Claims 7, 11-13 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Isikoff (U.S. Patent No. 5748084)* in view of *Hadfield et al. (Lee Hadfield, Dave Hater, Dave Bixler, "Windows NT Server 4 Security Handbook", 1997, ISBN: 078971213)* and *Patel et al. (U.S. Patent No. 6438690).*

Isikoff teaches a mobile system as discussed above using a GPS receiver and the transmitter transmitting its position coordinates (*Isikoff,* col. 10 lines 20-29).

Isikoff does not explicitly teach the security policies for the Pre-OS application and the OS-Present application including a designated number of failed log-on attempts, an unauthorized change attempted on selected platform policies, an unauthorized use of monitored services, a designated time expiration based on a renewable certificate, or a lack of communication to a policy server or to a security token, and an unauthorized deletion of the protected storage.

Hadfield et al. teach administrative security policy, account policy, audit policy and rights policy *(Hadfield et al. pg. 27-28)* which read on number of failed log-on, unauthorized use of monitored services and an unauthorized change attempted on selected platform policies.

Hadfiled et al. also teaches user rights permissions *(Hadfield et al. pg. 107),* which read on an unauthorized deletion of the protected storage.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include a designated number of failed log-on attempts, an unauthorized change attempted on selected platform policies, an unauthorized use of monitored services, and an unauthorized deletion of the protected storage into security polices for the Pre-OS application and the OS-Present application as taught by *Hadfield.* One of ordinary skill in the art would have been motivated to perform such a modification in order to specify how the users are allowed to interact with the system *(Handfield, pg. 27, last §).*

Isikoff also does not teach the security policies for the Pre-OS application and the OS-Present application including designated time expiration based on a renewable certificate.

Patel et al. teach certificate configuration policy *(Patel et al. col. 5 lines 38-46).* It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include a designated time expiration based on a renewable certificate into security polices for the Pre-OS application and the OS-Present application as taught by Patel et al. One of ordinary skill in the art would have been motivated to perform such a modification in order to increase the level of security *(Patel et al. col. 2 lines 4-12).*

27. Claims 8-10 and 17-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Isikoff (U.S. Patent No. 5748084)* in view of *Hadfield et al. (Lee Hadfield, Dave Hater, Dave Bixler, "Windows NT Server 4 Security Handbook", 1997, ISBN: 078971213)* and *Patel et al. (U.S. Patent No. 6438690)* and in further view of *Rainbow Technologies (Rainbow Technologies, "Protecting Laptops with iKey and Intel Protected Access Architecture").*

Isikoff teaches the mobile system as discussed above.

Isikoff does not explicitly a system basic input/output start-up being configured in accordance with IPAA and being executed during boot up before the OS is loaded.

Rainbow Technologies teach a system basic input/output start-up being configured in accordance with IPAA and being executed during boot up

before the OS is loaded *(Rainbow Technologies, "How Does IPAA Work section, pg. 2)*.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement a system basic input/output start-up being configured in accordance with IPAA and being executed during boot up before the OS is loaded as taught by *Rainbow Technologies*. One of ordinary skill in the art would have been motivated to perform such a modification in order to make a stolen laptop unusable *(Rainbow Technologies, The Intel Protected Access Architecture section, pg. 2)*.

Reporting any violation of the security policies would be implicit.

28. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over *Isikoff (U.S. Patent No. 5748084)* in *Isikoff (U.S. Patent No. 5748084)* in view of *Hadfield et al. (Lee Hadfield, Dave Hater, Dave Bixler, "Windows NT Server 4 Security Handbook", 1997, ISBN: 078971213)* and *Patel et al. (U.S. Patent No. 6438690)* and in further view of *Bajikar (U.S. Pub. 20020194500)*.

Isikoff teaches the mobile system as discussed above.

Isikoff does not teach the RF-based locator subsystem corresponding to a Bluetooth TM transceiver that is part of a Bluetooth TM based security system including a central security server and a network of Bluetooth (voice/data) Access Points (BTAPs) installed in a designated area to provide security services for the mobile system, including asset control, remote monitoring and tracking of the mobile system, through the Internet or the RF-based wireless network.

Bajikar teaches a Bluetooth based security system utilized to provide ad-hoc security services to secured assets comprising a secured device (SD) equipped with Bluetooth (BT) technology; a plurality of Bluetooth Access Points (BTAPs) located at designated points to establish a BT link with the secured device (SD); and a security server (SS) connected to all BTAPs and arranged to provide access control and security services for the secured device (SD), wherein the security server (SS) obtains attribute information *(Abstract and Fig. 1)*. Furthermore *Bajikar* discloses that the Bluetooth TM based security system serves to control and monitor the status of all secured devices or assets remotely, through the Internet or other networks *[0024]*. The *Bajikar's* teaching reads on RF-based locator subsystem corresponding to a Bluetooth TM transceiver that is part of a Bluetooth TM based security system including a central security server and a network of Bluetooth (voice/data) Access Points (BTAPs) installed in a designated area to provide security services for the mobile system, including asset control, remote monitoring and tracking of the mobile system, through the Internet or the RF-based wireless network.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to utilize a RF-based locator subsystem subsystem corresponding to a Bluetooth TM transceiver that is part of a Bluetooth TM based security system including a central security server and a network of Bluetooth (voice/data) Access Points (BTAPs) installed in a designated area to provide security services for the mobile system, including asset control,

remote monitoring and tracking of the mobile system, through the Internet or the RF-based wireless network as taught by *Bajikar.* One of ordinary skill in the art would have been motivated to perform such a modification in order to provide low-cost and low-power ad-hoc security *[Bajikar 0021].*

29. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over *Cromer et al. (U.S. Patent No. 6166688)* in view of *Isikoff (U.S. Patent No. 5748084).*

Cromer et al. teach the laptop with BIOS instructions as discussed above. *Cromer et al.* do not explicitly teach the system BIOS instructions to further cause the processor to report the location-based information indicating the current location of the mobile system to a proper authority, via an Internet or a RF-based wireless network, when there is a violation of the security policies. *Isikoff* teaches reporting the location-based information indicating the current location of the mobile system to a proper authority, via an Internet or a RF-based wireless network, when there is a violation of the security policies *(Isikoff col 2 lines 7-20).*

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to configure system BIOS instructions further cause the processor to report the location based information indicating the current location of the mobile system to a proper authority, via an Internet or a RF-based wireless network, when there is a violation of the security policies. *Isikoff* teach reporting the location-based information indicating the current location of the mobile system to a proper authority, via an Internet or a RF-

based wireless network, when there is a violation of the security policies as taugh by *Isikoff.* One of ordinary skill in the art would have been motivated to perform such a modification in order to recover a stolen laptop and capture of the thief *(Isikoff col. 2 lines 60-66).*

30. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over *Cromer et al. (U.S. Patent No. 6166688)* in view of *Hadfield et al. (Lee Hadfield, Dave Hater, Dave Bixler, "Windows NT Server 4 Security Handbook", 1997, ISBN: 078971213)* and *Patel et al. (U.S. Patent No. 6438690).*

Cromer et al. laptop computer with BIOS instructions as discussed above. *Cromer et al.* do not explicitly teach the security policies for the system BIOS instructions include a designated number of failed log-on attempts, an unauthorized change attempted on selected platform policies, an unauthorized use of monitored services, and an unauthorized deletion of a protected storage.

Hadfield et al. teach administrative security policy, account policy, audit policy and rights policy *(Hadfield et al. pg. 27-28)* which read on number of failed log-on, unauthorized use of monitored services and an unauthorized change attempted on selected platform policies. *Hadfield et al.* also teaches user rights permissions *(Hadfield et al. pg. 107),* which read on an unauthorized deletion of the protected storage.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include a designated number of failed log-on attempts,

an unauthorized change attempted on selected platform policies, an unauthorized use of monitored services, and an unauthorized deletion of the protected storage into the security policies for the system BIOS instructions as taught by *Hadfield et al.* One of ordinary skill in the art would have been motivated to perform such a modification in order to specify how the users are allowed to interact with the system *(Hadfield, pg. 27, last §)*.

Cromer et al. also do not teach the security policies for the Pre-OS application and the OS-Present application including a designated time expiration based on a renewable certificate.

Patel et al. teach certificate configuration policy (Patel et al. col. 5 lines 38-46).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include a designated time expiration based on a renewable certificate into security polices for the system BIOS instructions as taught by *Patel et al.* One of ordinary skill in the art would have been motivated to perform such a modification in order to increase the level of security *(Patel et al. col. 2 lines 4-12)*.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571)272-3840. The examiner can normally be reached

Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571)272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell
Andrew Caldwell

Signature

11/24/04

Date